IN THE CLAIMS

This listing of the claim will replace all prior versions and listings of claim in the present application.

Listing of Claims

1. (currently amended) An information processing method for calculating x*(2^n) mod P for an input value x larger than a prime number P, the operator ^ denoting power, said information processing method being executed by an information processing apparatus comprising a first memory of n bits sufficient for storing the modulus P, a second memory of m bits sufficient for storing said input value x, a third memory for storing 2^(2m+n) mod P and a Montgomery modular multiplication device, said information processing method comprising the steps of~~wherein~~:

~~the value x*(2^n) mod P is calculated without explicitly obtaining x mod P, by:~~ storing said input value x in said first memory of n bits;

calculating ~~or previously preparing~~ 2^(2m+n) mod P or reading said~~when the input value x has to be transformed into x*(2^n)~~ 2^(2m+n) mod P from said third memory by said Montgomery modular multiplication device;

reading said input value x from said first memory of n bits;

~~, the number n denoting the number of bits necessary and sufficient for storing the modulus P and the number m denoting the number of bits necessary for storing the input value x;~~

calculating x1 = x*2^(2m+n)*(2^(-m)) mod P = x*2^(m+n) mod P by said Montgomery modular multiplication device; ~~and~~

calculating x2 = x1*(2^(-m)) mod P = x*(2^n) mod P to transfer said input value x into x*(2^n) mod P without explicitly obtaining x mod P; and

storing said transferred value.

2. (currently amended) An information processing method for calculating x*(2^n) mod P for an input value x larger than a prime number P, the operator ^ denoting power, said information processing method being executed by an information processing apparatus comprising a first memory of n bits sufficient for storing the modules P, a second memory of m bits sufficient for storing said input value x, a third memory for storing 2^(m+2n) mod P and a Montgomery modular multiplication device, said information processing method comprising the steps ofwherein: ~~the value x*(2^n) mod P is calculated without explicitly obtaining x mod P, by:~~

storing said input value x in said first memory of n bits;

calculating ~~or previously preparing~~ 2^(m+2n) mod P or reading said 2^(m+2n) mod P from said third memory by said Montgomery modular multiplication device;

reading said input value x from sadi first memory of n bits;

~~when the input value x has to be transformed into x*(2^n) mod P, the number n denoting the number of bits necessary and sufficient for storing the modulus P and the number m denoting the number of bits necessary for storing the input value x;~~

calculating x1 = x*2^(m+2n)*(2^(-m)) mod P = x*2^(2n) mod P by said Montgomery modular multiplication device; and

calculating x2 = x1*(2^(-n)) mod P = x*(2^n) mod P to transfer said input value x into x*(2^n) mod P without explicitly obtaining x mod P; and

storing said transferred value.

Claim 3 (canceled).

4. (currently amended) The information processing method of claim 1 for an RSA cryptosystem method using Chinese Remainder Theorem, said method comprising the steps of:

~~inputting an input value X;~~

calculating mod P using the information processing method according to claim 1 and encrypting said input value ~~the~~ x; and

storing said ~~the~~ encrypted input value x.

5. (currently amended) The information processing method of claim 2 for an RSA cryptosystem method using Chinese Remainder Theorem, said method further comprising the steps of:

~~inputting an input value X;~~

calculating mod P using the information processing method according to claim 2, and encrypting said input value ~~the~~ x; and

storing said ~~the~~ encrypted input value x.

6. (currently amended) An information processing apparatus for calculating x*(2^n)mod P for an input value x larger than a prime number P, the operator ^ denoting power, said apparatus comprising:

a memory of n bits~~wherein the number n denotes the number of bits necessary and~~ sufficient for storing the modulus P;

a memory of m bits sufficient for ~~and the number m denotes the number of bits necessary for~~ storing ~~the~~ said input value x, and

a ~~wherein the information processing apparatus comprises~~ Montgomery modular multiplication device, wherein said ~~and the~~ Montgomery modular multiplication device adapted to execute the steps of

calculating 2^(2m+n) mod P;

reading said input value x from said memory of n bits; and

calculating ~~es~~ x1=x*2^(2m+n)*(2^(-m)) mod P=x*2^(m+n) mod P

and ~~calculates~~ x2=x1*(2^(-m)) mod P = x*(2^n) mod P to transfer said input value x into x*(2^n) mod P without explicitly obtaining x mod P.